IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

1. (CURRENTLY AMENDED) An encryption circuit that generates from a cipher key a plurality of round keys having a number of bits corresponding to a predetermined processing block length and executing, for each processing block length, input data and round key encryption/decryption processing, by means of a round function unit comprising an XOR operation unit that XORs the input data and one of the round keys and

a round processing unit that iterates round processing that includes Byte Sub transformation, ~~Shift Row transformation,~~ Mix Column transformation and Round Key Addition, which are executed at execution block length that is smaller than said predetermined processing block length, the round processing further including Shift Row transformation which is performed on data having the predetermined processing block length, wherein:

said round processing unit comprises:

a first selector that segments input data having the predetermined processing block length into data segments having the execution block ~~lengths smaller than said processing block~~ length;

a first Round Key Addition circuit that adds said round key value to input data for each said execution block length;

an intermediate register/Shift Row transformation circuit that temporarily stores the output of said first Round Key Addition circuit and executes Shift Row transformation using said predetermined processing block length;

a Byte Sub transformation circuit wherein said intermediate register/Shift Row transformation circuit value is inputted for each said execution block length and Byte Sub transformation is executed;

a second Round Key Addition circuit wherein

said intermediate register/Shift Row transformation circuit value is inputted for each said execution block length and said round key value is added for each said execution block length;

a Mix Column transformation circuit executing Mix Column transformation on the output of said second Round Key Addition circuit; and

a second selector that outputs to said first Round Key Addition circuit one output from

among the outputs of said first selector, intermediate register/Shift Row transformation circuit, Byte Sub transformation circuit, or Mix Column transformation circuit, the second selector enabling the first Round Key Addition circuit, the Byte Sub transformation circuit and the Mix Column transformation circuit to perform continuously at the execution block length without an extra processing circuit.

2. (ORIGINAL) An encryption circuit according to claim 1 wherein said execution block length is a multiple of 8 bits.

3. (ORIGINAL) An encryption circuit according to claim 1, wherein said processing block length is 128 bits and said execution block length is 32 bits.

4. (ORIGINAL) An encryption circuit according to claim 1, wherein the key length of the cipher key is any of 128 bits, 192 bits or 256 bits.

5. (ORIGINAL) An encryption circuit according to claim 1, wherein:

said Byte Sub transformation circuit comprises a matrix operation unit for decryption that executes a matrix operation on input data;

a third selector that outputs either the input data or the output of said matrix operation unit for decryption;

an inverse operation unit for executing an inverse operation on the data outputted from said third selector; a matrix operation unit for encryption that executes a matrix operation on the data outputted from said inverse operation unit; and a fourth selector that outputs either the output of said inverse operation unit or the output of said matrix operation unit for encryption.

6. (ORIGINAL) An encryption circuit according to claim 5, wherein said matrix operation unit for decryption and said matrix operation unit for encryption comprises an XOR circuit so as to perform 8-bit operations at one clock cycle.

7. (ORIGINAL) An encryption circuit according to claim 5, wherein said matrix operation unit for decryption and said matrix operation unit for encryption comprises an XOR circuit so as to perform 1-bit operations at one clock cycle.

8. (ORIGINAL) An encryption circuit according to claim 1, wherein said intermediate

register/Shift Row transformation circuit can be used for both encryption and decryption through the reversal of order of input of shift data relating to amount of shift for data to be inputted into said intermediate register/Shift Row transformation circuit, the input order for decryption being the reverse of the order for encryption.

9. (ORIGINAL) An encryption circuit according to claim 1, wherein said Mix Column transformation circuit comprises a plurality of multiplication units with unique multipliers and an XOR circuit that performs XOR operations for said plurality of multiplication units, said Mix Column transformation circuit executing a matrix operation between data inputted into each multiplication unit and the multiplier established for each multiplication unit.

10. (ORIGINAL) An encryption circuit according to claim 9, wherein said Mix Column transformation circuit comprises 4 operation units having 4 multiplication units capable of 8-bit unit operations and XOR circuits that execute XOR operations based on the outputs of said 4 multiplication units.

11. (ORIGINAL) An encryption circuit according to claim 9, wherein said multiplication units can control 2 multipliers and are used for both encryption and decryption.

12. (ORIGINAL) An encryption circuit according to claim 11, wherein said multiplication units are constituted to control addition values from high-order bits.

13. (ORIGINAL) An encryption circuit according to claim 1 having a key expansion schedule circuit that generates from said cipher key, as an expanded key segmented into bit numbers corresponding to said execution block length, a plurality of round keys with bit numbers corresponding to a predetermined processing block length; the key expansion schedule circuit comprising:

a fifth selector that segments a cipher key into the number of bits corresponding to said execution block length and outputs the same;

a shift register to which flip-flop circuits are connected at a plurality of stages, said flip-flop circuits latching data in units of said execution block length;

a first XOR circuit that XORs the output of the final stage flip-flop circuit of said shift register with one constant selected from among a group of constants;

a sixth selector into which are inputted the outputs of those flip-flops of said shift register

that are involved in operations for encryption and the outputs of those flip-flops involved in operations for decryption, and which selectively outputs one of these;

a Rot Byte processing circuit that rotates the output of said sixth selector;

a seventh selector into which the output of said sixth selector and the output of said Rot Byte circuit is inputted and which selectively outputs one of these;

a Sub Byte processing circuit that executes Byte Sub transformation on the output of said seventh selector for each said execution block length;

an eighth selector into which the output of said sixth selector and the output of said Sub Byte processing circuit are inputted, and which selectively outputs one of these;

a second XOR circuit that executes an XOR operation based on the output of said first XOR circuit and the output of said eighth selector; and

a shift register unit selector that selectively outputs, to those flip-flops of said shift register the outputs of which are subject to operations for encryption, either the output of said second XOR circuit or the output of the adjacent stage flip-flop.

14. (ORIGINAL) An encryption circuit according to claim 13, wherein said shift register comprises 8 flip-flops executing data processing in 32-bit units, and said sixth selector is constituted so that the outputs of the second, fourth, sixth and eighth flip-flops from the bottom from among said flip-flops are inputted therein, and that it outputs one of these.

15. (ORIGINAL) An encryption circuit according to claim 13, wherein through the input into said seventh selector of the output of said intermediate register/Shift Row transformation circuit and the input into said second selector of the output of said Sub Byte processing circuit, a single circuit can be used for said Sub Byte processing circuit and said Byte Sub transformation circuit of said round processing unit.

16. (NEW) An encryption circuit for implementing in hardware AES, the encryption circuit comprising:

a key schedule unit that generates a plurality of round keys from a cipher key, each round key having a processing block length; and

a round function unit performing input data and round key encryption/decryption processing for each processing block length, the round function unit comprising:

a first selector that segments input data having processing block length into input data segments having execution block length which is smaller than said processing block

length;

an XOR operation unit that XORs the input data and one of the round keys; and

a plurality of round processing units to iterate round processing that includes Byte Sub transformation, Shift Row transformation, Mix Column transformation and Round Key Addition, wherein each round processing unit comprises:

a first Round Key Addition circuit that adds said round key to input data segments having said execution block length;

an intermediate register/Shift Row transformation circuit that temporarily stores an output of said first Round Key Addition circuit and executes Shift Row transformation using said processing block length;

a Byte Sub transformation circuit wherein a segmented output of said intermediate register/Shift Row transformation circuit is input for each said execution block length and Byte Sub transformation is executed;

a second Round Key Addition circuit wherein the segmented output of said intermediate register/Shift Row transformation circuit is input for each said execution block length and said round key is added for each said execution block length;

a Mix Column transformation circuit executing Mix Column transformation on the output of said second Round Key Addition circuit; and

a second selector that outputs to said first Round Key Addition circuit one output from outputs of said first selector, intermediate register/Shift Row transformation circuit, Byte Sub transformation circuit, or Mix Column transformation circuit.

17. (NEW) An encryption circuit according to claim 16, wherein said Byte Sub transformation circuit comprises:

a matrix operation unit for decryption that executes a matrix operation on input data;

a third selector that outputs either the input data or the output of said matrix operation unit for decryption;

an inverse operation unit for executing an inverse operation on the data outputted from said third selector;

a matrix operation unit for encryption that executes a matrix operation on the data outputted from said inverse operation unit; and

a fourth selector that outputs either the output of said inverse operation unit or the output

of said matrix operation unit for encryption.

18. (NEW) An encryption circuit according to claim 16, the key schedule unit comprising:

a fifth selector that segments a cipher key into the number of bits corresponding to said execution block length and outputs the same;

a shift register to which flip-flop circuits are connected at a plurality of stages, said flip-flop circuits latching data in units of said execution block length;

a first XOR circuit that XORs the output of the final stage flip-flop circuit of said shift register with one constant selected from among a group of constants;

a sixth selector into which are inputted the outputs of those flip-flops of said shift register that are involved in operations for encryption and the outputs of those flip-flops involved in operations for decryption, and which selectively outputs one of these;

a Rot Byte processing circuit that rotates the output of said sixth selector;

a seventh selector into which the output of said sixth selector and the output of said Rot Byte circuit is inputted and which selectively outputs one of these;

a Sub Byte processing circuit that executes Byte Sub transformation on the output of said seventh selector for each said execution block length;

an eighth selector into which the output of said sixth selector and the output of said Sub Byte processing circuit are inputted, and which selectively outputs one of these;

a second XOR circuit that executes an XOR operation based on the output of said first XOR circuit and the output of said eighth selector; and

a shift register unit selector that selectively outputs, to those flip-flops of said shift register the outputs of which are subject to operations for encryption, either the output of said second XOR circuit or the output of the adjacent stage flip-flop.

19. (NEW) An encryption circuit according to claim 18, wherein said shift register comprises 8 flip-flops executing data processing in 32-bit units, and said sixth selector is constituted so that the outputs of the second, fourth, sixth and eighth flip-flops from the bottom from among said flip-flops are inputted therein, and that it outputs one of these.

20. (NEW) An encryption circuit according to claim 18, wherein through the input into said seventh selector of the output of said intermediate register/Shift Row transformation circuit and the input into said second selector of the output of said Sub Byte processing circuit, a single circuit can be used for said Sub Byte processing circuit and said Byte Sub transformation circuit

of said round processing unit.